

CYBER 4.0, 18 APRILE 2025

Cyber 4.0 ha un nuovo Presidente: la nomina di Paolo Spagnoletti

Il 10 di aprile 2025 l'Assemblea dei soci ha votato per l'elezione della nuova governance del Centro di Competenza Cyber 4.0. I nuovi eletti resteranno in carica per il **triennio 2025-2027**. All'ex Presidente Leonardo Querzoni, subentra Paolo Spagnoletti, Professore Ordinario di Organizzazione Aziendale presso la Luiss Guido Carli University. Spagnoletti porta con sé una solida esperienza accademica e una visione strategica sul futuro digitale del Paese.



[LEGGI TUTTO](#)

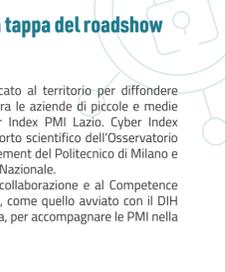
Articoli Correlati:

[Il Giornale, Cyber 4.0 ha un nuovo presidente: la nomina di Paolo Spagnoletti, 18 Aprile 2025](#)

MINISTERO DELLE IMPRESE E DEL MADE IN ITALY, 7 APRILE 2025

Cybersecurity, Urso firma protocollo d'intesa Mimit-ACN per rafforzare tutela di imprese e PA

È stato firmato a Palazzo Piacentini, dal ministro delle Imprese e del Made in Italy, Adolfo Urso, e dal direttore generale dell'Agenzia per la cybersecurity nazionale, prefetto Bruno Frattasi, un protocollo d'intesa tra il Mimit e ACN per avviare una collaborazione strutturata e continuativa sugli European Digital Innovation Hub. Nel dettaglio, il protocollo, ha l'obiettivo di facilitare azioni di intervento mirate sui territori che consentano al Mimit di rafforzare le filiere strategiche, rendendo stabile e continuativa l'interazione con la rete degli EDIH.



[LEGGI TUTTO](#)

CYBER 4.0

LA REPUBBLICA, 1 APRILE 2025

Generali-Confindustria: a Roma nuova tappa del roadshow dedicato a cultura gestione cyber risk

A Roma la prima tappa dell'anno del roadshow dedicato al territorio per diffondere e promuovere la cultura della gestione del cyber risk tra le aziende di piccole e medie dimensioni, con la presentazione del Rapporto Cyber Index PMI Lazio. Cyber Index PMI, realizzato da Generali e Confindustria, con il supporto scientifico dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano e con la partecipazione dell'Agenzia per la Cybersecurity Nazionale. Grazie alla nostra rete istituzionale sul territorio, alla collaborazione e al Competence Center Cyber 4.0, stiamo sviluppando percorsi specifici, come quello avviato con il DIH Lazio nell'ambito del progetto Confinhub di Confindustria, per accompagnare le PMI nella transizione digitale sicura in un'ottica di filiera.

[LEGGI TUTTO](#)

SAPIENZA UNIVERSITÀ DI ROMA, 9 APRILE 2025

Il Segretario di Stato per gli affari esteri del Regno Unito David Lammy in visita alla Sapienza

Il Segretario di Stato per gli Affari Esteri del Regno Unito, David Lammy, ha visitato l'Università La Sapienza di Roma. Durante l'incontro con il Rettore e le autorità accademiche, il Ministro ha dialogato con i ricercatori impegnati su progetti innovativi nell'ambito dell'AI, discutendo anche sui temi di cooperazione internazionale e ricerca. La visita sottolinea l'importanza delle relazioni accademiche tra Italia e Regno Unito.

[LEGGI TUTTO](#)

IN ITALIA

CYBERSECURITY ITALIA, 3 APRILE 2025

"Un comando unificato gestito dalla Difesa in caso di cyber attacchi". La proposta della Commissione Difesa della Camera

La Commissione Difesa della Camera dei deputati ha approvato all'unanimità un documento strategico sulla difesa cibernetica. Il testo propone la creazione di un comando unificato gestito dalla Difesa per rispondere tempestivamente agli attacchi informatici, proteggendo le infrastrutture civili e militari. Inoltre, enfatizza l'importanza della formazione e sensibilizzazione sulla cybersecurity, integrando la materia nei percorsi scolastici e promuovendo la collaborazione tra pubblico e privato.

[LEGGI TUTTO](#)

CIS-SAPIENZA & CYBERSECURITY NATIONAL LAB-CINI, APRILE 2025

Framework Nazionale per la Cybersecurity e la Data Protection - Edizione 2025

Il Framework Nazionale per la Cybersecurity e la Data Protection, viene oggi proposto con una nuova versione che allinea il suo core a quello del NIST CSF. Frutto di una collaborazione tra il Centro di Ricerca CIS di Sapienza Università di Roma ed il Laboratorio Nazionale di Cybersecurity del CINI, con il supporto dell'Agenzia per la Cybersecurity Nazionale, questa nuova versione del Framework Nazionale per la Cybersecurity e la Data Protection permette alle organizzazioni di lavorare con uno strumento allineato alle best practice internazionali e coerente con le correnti normative di settore.

[LEGGI TUTTO](#)

CYBER SECURITY 360, 14 APRILE 2025

NIS2, arrivano le PEC dall'ACN: ecco cosa devono fare subito le aziende coinvolte

A partire dal 12 aprile 2025, l'Agenzia per la Cybersecurity Nazionale (ACN) ha iniziato a notificare ufficialmente, tramite PEC, l'inclusione dei soggetti registrati nell'elenco degli operatori regolati dal Decreto Legislativo 123/2023, ovvero quelli rientranti a pieno titolo nell'ambito di applicazione nazionale della direttiva NIS2, che impone nuovi obblighi in materia di sicurezza digitale. Entro il 28 febbraio 2025 le imprese avevano l'obbligo di registrarsi sul portale ACN, fornendo dati su struttura, settore e responsabilità di cybersecurity. Chi non adempie rischia sanzioni fino allo 0,1% del fatturato annuo.

[LEGGI TUTTO](#)

ACN, 9 APRILE 2025

Vicenda telefoni e dati dei vip - Nota Stampa

In giornata è stata diffusa da alcune testate radio televisive, la notizia secondo cui l'Agenzia per la cybersecurity nazionale avrebbe appreso, da una segnalazione informale avvenuta sul noto social LinkedIn, della esposizione sul web dei numeri personali di alte cariche dello Stato e che a tale segnalazione non sia stato dato il seguito necessario, visto il rilievo delle figure istituzionali interessate.

[LEGGI TUTTO](#)

CYBERSECURITY ITALIA, 14 APRILE 2025

Ransomware, la proposta di legge Mauri: divieto di pagamento, obbligo di notifica e fondo per le aziende colpite

La crescente minaccia ransomware è entrata finalmente al centro del dibattito legislativo italiano. Lo scorso 20 marzo è stata depositata alla Camera dei deputati la proposta di legge a firma dell'on. Matteo Mauri (PD), che punta a dotare il Paese di una strategia nazionale strutturata per contrastare questo fenomeno sempre più pervasivo e pericoloso. Il testo, articolato in un unico articolo che delega il Governo a intervenire con decreti legislativi entro sei mesi, si basa su nove direttrici fondamentali, configurandosi come un primo, importante passo verso una resilienza nazionale strutturata e condivisa.

[LEGGI TUTTO](#)

IL SOLE 24 ORE, 5 APRILE 2025

Spazio in sole Starlink: in arrivo i 100 satelliti per la sicurezza dell'Italia

L'Italia progetta, e pensa di realizzare in pochi anni, una costellazione di satelliti per telecomunicazioni legate alla sicurezza e alla difesa. Uno studio di fattibilità, preparato dall'Agenzia Spaziale Italiana. Asi, è stato infatti consegnato nelle settimane scorse al Ministero delle Imprese e del Made in Italy. Nel rapporto Asi si prevede una costellazione di almeno cento satelliti, che potrebbe essere pronta in almeno cinque anni.

[LEGGI TUTTO](#)

NEWS INTERNAZIONALI

AGENZIA PER LA CYBERSICUREZZA NAZIONALE, 10 APRILE 2025

Presentato il piano UE per potenziare l'applicazione degli strumenti di AI nelle imprese

È stato presentato ieri, dal Vicepresidente della Commissione europea Henna Maria Virkkunen, l'AI Continent Action Plan: un programma per rafforzare l'adozione dell'intelligenza artificiale (AI) nelle imprese europee. Fondamentale, in questo contesto, il ruolo dell'Italia con la realizzazione di ITALIA, una delle due AI Factory Europee, fra le 13 presentate, oltre a quella finlandese, che prevede l'acquisizione di un supercomputer ottimizzato per applicazioni di Intelligenza artificiale.

[LEGGI TUTTO](#)

EUROPEAN COMMISSION, APRIL 11, 2025

Commission opens consultation on revising EU Cybersecurity Act

In an effort to strengthen the EU's resilience against rising cyber threats, the Commission seeks input to evaluate and revise the 2019 Cybersecurity Act. This initiative reflects the Commission's ongoing commitment to simplifying rules.

[LEGGI TUTTO](#)

EUR-LEX, APRIL 1ST, 2025

Communication from The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee of The Regions on ProtectEU: a European Internal Security Strategy

The European Commission has published the "ProtectEU" strategy, aiming to strengthen internal security across the EU. The initiative outlines key priorities to enhance digital access to justice, promote cross-border judicial cooperation, and encourage the adoption of innovative technologies such as AI. It also seeks to close the digital divide and improve user experience within justice systems. Measures include upgrading the e-Justice Portal, introducing real-time tools like video conferencing, and increasing transparency through data-driven solutions. The strategy reflects a broader commitment to making justice more efficient, accessible, and resilient in the digital age.

[LEGGI TUTTO](#)

EUROPOL, APRIL 2, 2025

Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users

Kidflix, one of the largest paedophile platforms in the world, has been shut down in an international operation against child sexual exploitation. The investigation was supported by Europol and led by the State Criminal Police of Bavaria (Bayerisches Landeskriminalamt) and the Bavarian Central Office for the Prosecution of Cybercrime (ZCB). Over 35 countries worldwide participated in the operation.

[LEGGI TUTTO](#)

ENISA, APRIL 2, 2025

First EUCC Cybersecurity Certificates Set Sails from France

ANSSI, the French cybersecurity agency, has just issued the first two EU cybersecurity certificates under EUCC. Prepared by ENISA and adopted by the European Commission on 27 February 2024, the EU Common Criteria scheme, EUCC, is the first EU cybersecurity scheme in place. As from 27 February this year, Member States can deliver EUCC certificates.

[LEGGI TUTTO](#)

THE RECORD, APRIL 11TH, 2025

Morocco investigates major data breach allegedly by Algerian hackers

Morocco's national social security agency is investigating a cyberattack that resulted in the leak of sensitive personal data reportedly belonging to millions of citizens. The National Social Security Fund of Morocco (CNSS), which oversees healthcare, disability, and retirement benefits for the country's private-sector employees, said hackers bypassed its security systems and leaked some of the agency's data. More than 54,000 files were allegedly stolen, exposing information on nearly 2 million people, according to Moroccan media reports.

[LEGGI TUTTO](#)

EUROPOL, APRIL 9, 2025

Operation Endgame follow-up leads to five detentions and interrogations as well as server takedowns

Following the massive botnet takedown codenamed Operation Endgame in May 2024, which shut down the biggest malware droppers, law enforcement agencies across North America and Europe dealt another blow to the malware ecosystem in early 2025. Law enforcement moved against the criminals who used the services taken down during Operation Endgame, focusing on the demand side of the criminal ecosystem. In a coordinated series of actions, customers of the SmokeLoader pay-per-install botnet, operated by the actor known as 'Superstar', faced consequences such as arrests, house searches, arrest warrants or 'knock and talks'.

[LEGGI TUTTO](#)

GOOGLE CLOUD, APRIL 1, 2025

DPRK IT Workers Expanding in Scope and Scale

Since our September 2024 report outlining the Democratic People's Republic of Korea (DPRK) IT worker threat, the scope and scale of their operations has continued to expand. These individuals pose as legitimate remote workers to infiltrate companies and generate revenue for the regime. This places organizations that hire DPRK IT workers at risk of espionage, data theft, and disruption.

[LEGGI TUTTO](#)

SECURITYWEEK NETWORK, APRIL 11, 2025.

China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report

In a secret meeting that took place late last year between Chinese and American officials, the former confirmed that China had conducted cyberattacks against US infrastructure as part of the campaign known as Volt Typhoon, according to The Wall Street Journal. The conclusion of American officials after the meeting was that the cyberattacks were meant to scare the United States from getting involved in a potential conflict between China and Taiwan.

[LEGGI TUTTO](#)

Nuove Pubblicazioni

[AI Privacy Risks & Mitigations Large Language Models \(LLMs\) - European Data Protection Board, April 10, 2025](#)

[Threat Research Team- Sublime Security, TROY Stealer: A deep dive into a new Malware as a Service \(MaaS\) attack campaign, April 10, 2025](#)

[Cyble, ICS Vulnerability Report: Energy, Manufacturing Device Fixes Urged by Cyble, April 10, 2025](#)

[CAIDP, The AI Policy Sourcebook 2025, April 2, 2025.](#)

Prossimi Eventi

[RSAC Conference, RSA Conference, 2025, April 28- May 1, 2025, Moscone Center, San Francisco.](#)

[TIG- The Innovation Group, Healthcare Innovation Executive Conference, 6 maggio 2025, dalle ore 09:30, The Hive Hotel, Roma.](#)

[SOIEL International, Sicurezza ICT 2025, 7 maggio 2025, dalle ore 09:30, Precise House Mantegna, Roma.](#)

[Cyber 4.0, Forum Cyber 4.0 2025, 4-5 giugno 2025, Università degli Studi Roma Tre, Aula Magna del Rettorato, Roma.](#)